CAREER: Towards Secure Augmented Reality Platforms

Challenge:

Emerging augmented reality (AR) technologies raise new and serious computer security and privacy risks—risks that arise for AR input (due to the need for continuous sensing), AR output (buggy or malicious applications affecting a user's view of the physical world), as well as multi-app and and multi-user interactions.

Scientific Impact:

This project has had direct impacts on the field of computer security and privacy by advancing our understanding of the challenges and risks with emerging AR technologies, as well as potential solutions. These advances will lay a foundation for future AR technologies to balance exciting and useful new functionality with the security, privacy, and safety of end users.

Solution:

- Approach: Combination of threat modeling, user studies, analysis of commercially available platforms, and system design and prototyping
- Key findings and innovations: AR output security module; multi-user AR content sharing library; multi-app designs; empirical evidence of attack impacts on people; attacks enabled by of current platforms

Broader Impact and Broader Participation:

- Engagement with key industry players, including Apple, Google, Meta, Microsoft, Niantic, etc. (e.g., Industry-Academic Summit, student placement, presentations, conversations)
- Release of ShareAR multi-user AR sharing toolkit
- Graduate and undergraduate research opportunities

Franziska Roesner
franzi@cs.washington.edu
Award Number CNS-1651230

PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING